AMENDMENTS TO THE SPECIFICATION:

Please amend the specification as follows.

At page 8, lines 16-18:

Figure 2 ~~2A~~ is a flow diagram showing the process of verifying that a card is authentic, or at worst an exact clone of an authentic card, and checking if the card is not in the list of cards to be refused;

At page 8, line 19:

~~Figure 2B is a flowchart showing the steps corresponding to the flow of Figure 2A;~~

At page 10, lines 4-7:

The concatenation on 101 and 102 forms l1 at 103. Then, a function f which is invertible and will be publicly known is chosen, and one constructs l2 = f(l1) at 104, l3 = f(l2) at 105, l4 = f(l3) at 106 and so forth. The function f, for example, can be chosen to be the identity map, in which case l1 = l2 = l3 = ...etc.

At page 10, lines 8-12:

For some number N, typically of the order of 100 or more, N public key-private key pairs are chosen. It is noted that, the more pairs there are, the greater the security. As mentioned above, if the card is used frequently, then more key pairs would be desired. The first private key V1 at 113 is used to compute h1 = V1(l1) at 123, the second private key V2 at 114 is used to

compute h2 = V2(l2) at 124, the third private key V3 at 115 is used to compute h3 = V3(l3) at 125, the fourth private key V4 at 116 is used to compute h4 = V4(l4) at 126, and so on.

At page 11, line 16, to page 12, line 8:

For example, as illustrated in Figure 3, a typical hardware configuration of an information handling/computer system for use with the invention is shown. In accordance with the invention, preferably the system has at least one processor or central processing unit (CPU) 311 and more preferably several CPUs 311. The CPUs 311 are interconnected via a system bus 312 to a random access memory (RAM) 314, read-only memory (ROM) 316, input/output (I/O) adapter 318 (for connecting peripheral devices such as disk units 321 and tape drives 340 to the bus 312), user interface adapter 322 (for connecting a keyboard 324, an input device such as a mouse, trackball, joystick, touch screen, etc. 326, speaker 328, microphone 332, and/or other user interface device to the bus 312), communication adapter 341 ~~334~~ (for connecting the information handling system to a data processing network such as an intranet, the Internet (World-Wide-Web) etc.), and display adapter 336 (for connecting the bus 312 to a display device 338). The display device could be a cathode ray tube (CRT), liquid crystal display (LCD), etc., as well as a hard-copy printer (e.g., such as digital printer). Further, a reader 342 is coupled to the CPU 311 via bus 312.

At page 14, line 17, to page 15, line 2:

Further, the smart cards do not carry confidential information thereon and the smart cards are difficult to duplicate/counterfeit. Indeed, there is no key at all held in the card. The card merely holds two related words (e.g., a pair including the suffix and the sequence) as a secret.

Instead, the reader holds the key (e.g., the public key) therein along with a database which, as mentioned above, is updated periodically. The database holds information representing disallowed/refused cards possibly ~~possible~~ representing that the cards have been stolen, voluntarily discontinued by the legitimate owner, etc.